UNITED STATES PATENT AND TRADEMARK OFFICE

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/943,889	08/31/2001	Shigeru Morino	01533/LH	2070

			EXAMINER
1933	7590	03/28/2005	HA, LEYNNA A

FRISHAUF, HOLTZ, GOODMAN & CHICK, PC
767 THIRD AVENUE
25TH FLOOR
NEW YORK, NY 10017-2023

ART UNIT	PAPER NUMBER
2135	

DATE MAILED: 03/28/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)
	09/943,889	MORINO, SHIGERU
	Examiner	Art Unit
	LEYNNA T. HA	2135

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE <u>3</u> MONTH(S) FROM
THE MAILING DATE OF THIS COMMUNICATION.
- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed
  after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
  Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any
  earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☐ Responsive to communication(s) filed on _____.

2a)☐ This action is **FINAL**.   2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is
closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-9* is/are pending in the application.

    4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-9* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

    Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

    Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

    a)☐ All   b)☐ Some * c)☐ None of:

      1.☐ Certified copies of the priority documents have been received.

      2.☐ Certified copies of the priority documents have been received in Application No. _____.

      3.☐ Copies of the certified copies of the priority documents have been received in this National Stage
application from the International Bureau (PCT Rule 17.2(a)).

    * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1)☒ Notice of References Cited (PTO-892)

2)☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3)☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date <u>08/31/2001</u>.

4)☐ Interview Summary (PTO-413)
    Paper No(s)/Mail Date. _____ .

5)☐ Notice of Informal Patent Application (PTO-152)

6)☐ Other: _____ .

DETAILED ACTION

1.   Claims 1-9 have been examined and are rejected under 35

U.S.C. 103(a).

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for

all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or
> described as set forth in section 102 of this title, if the differences between the
> subject matter sought to be patented and the prior art are such that the subject
> matter as a whole would have been obvious at the time the invention was made to a
> person having ordinary skill in the art to which said subject matter pertains.
> Patentability shall not be negatived by the manner in which the invention was made.

2.   Claims 1-19 are rejected under 35 U.S.C. 103(a) as being

unpatentable over Rosner, et al. (US 6,636,968).

As per claim 1:

Rosner, Et al. discloses a method for encrypting and decrypting contents

data to be distributed from a server to a user terminal through a

network, said method comprising:

generating a first key at the server from contents information

about the distributed contents data; **(col.3, lines 51-60)**

generating a second key at the server from a variable parameter, a

H/W key ID **(col.5, lines 1-6)**, and said first key and sending the

generated second key to the user terminal; **(col.3, lines 8-11 and col.4, lines 37-45)**

encrypting the contents data to be distributed at the server by using said first key and sending the encrypted contents data to the user terminal; and **(col.4, lines 13-30)**

decrypting the encrypted contents data at the user terminal by using said decrypted first key. **(col.5, lines 10-33)**

Rosner discusses the decryption key was formed from the a partial key, group key, and combined with a private key of each H/D **(col.4, lines 30-35)** where that was used to encrypt the content material **(col.5, lines 22-35)**. Hence, it is obvious decrypting the first key from the variable parameter, the H/W key ID, and said second key is necessary to obtain the encrypted content.

As per claim 2:   See col.2, lines 56-61; discussing generating the variable parameter at the user terminal and sending the generated variable parameter to the server.

As per claim 3:   See col.3, lines 42-50; discussing the variable parameter used for generating the second key at the server are the variable parameter sent from the user terminal.

As per claim 4:   See col.4, lines 12-23; discussing synchronizing the variable parameter between the user terminal and the server.

As per claim 5:   See col.3, lines 63-67; discussing synchronization between the user terminal and the server is performed at a time different from a time when the contents data is distributed.

As per claim 6:

Rosner discloses contents data encrypting and decrypting system comprising:

a server, the server comprising;

means for generating a first key from contents information of contents data to be distributed , means for generating a second key from a variable parameter, a H/W key ID **(col.5, lines 1-6)**, and said first key, and means for encrypting the contents data to be distributed by using the first key; and **(col.3, lines 42-45 and lines 51-60)**

a user terminal, the user terminal comprising;

a network interface configured to receive said second key and said encrypted contents data from said server, means for decrypting the first key from the variable parameter, the H/W key ID, and said second key **(col.4, lines 8-35 and lines 48-57)**, and means for decrypting said encrypted contents data by using said decrypted first key. **(col.5, lines 10-33)**

Rosner discusses the decryption key was formed from the a partial key, group key, and combined with a private key of each H/D **(col.4, lines 30-35)** where that was used to encrypt the content material **(col.5, lines 22-35)**. Hence, it is obvious decrypting the first key from the

variable parameter, the H/W key ID, and said second key is necessary to obtain the encrypted content.

As per claim 7:   See col.3, lines 63-67; discussing means for synchronizing the variable parameter between said server and said user terminal.

As per claim 8:

Rosner discloses a user terminal used for encrypting and decrypting contents data to be distributed from a server through a network, the user terminal comprising:

a network interface configured to receive from the server a second key generated from a first key generated from contents information of the contents data to be distributed, a variable parameter, and a H/W key ID **(col.5, lines 1-6)**, and the contents data encrypted by using said first key; and **(col.3, lines 42-45 and lines 51-60)**

a decrypting section configured to decrypt the first key from the variable parameter, the H/W key ID, and said second key **(col.4, lines 8-35 and lines 48-57)**, and then decrypt said encrypted contents data by using said decrypted first key. **(col.5, lines 10-38)**

As per claim 9:   See col.3, lines 63-67; discussing the user terminal further comprising means for synchronizing the variable parameter between the server and the user terminal.

Rosner discusses the decryption key was formed from the a partial key, group key, and combined with a private key of each H/D **(col.4,**

lines 30-35) where that was used to encrypt the content material **(col.5, lines 22-35)**. Hence, it is obvious decrypting the first key from the variable parameter, the H/W key ID, and said second key is necessary to obtain the encrypted content.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to LEYNNA T. HA whose telephone number is (571) 272-3851. The examiner can normally be reached on Monday - Thursday (7:00 - 5:00PM).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on (571) 272-3859. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained

from the Patent Application Information Retrieval (PAIR) system. Status

information for published applications may be obtained from either

Private PAIR or Public PAIR. Status information for unpublished

applications is available through Private PAIR only. For more

information about the PAIR system, see http://pair-direct.uspto.gov.

Should you have questions on access to the Private PAIR system, contact

the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

LHa

AU 2135